telecomkh.com

http://www.telecomkh.com/en/internet/9043
From raw data to actionable intelligence: The art and science of endpoint security
27/04/17

Date: ***Thu, 04/27/2017 - 11:27*** Source: By Alan Zeichick

The endpoint is vulnerable. That's where many enterprise cyberbreaches begin: An employee clicks on a phishing link and installs malware, such a ransomware, or is tricked into providing login credentials. A browser can open a webpage which installs malware. An infected USB flash drive is another source of attacks. Servers can be subverted with SQL Injection or other attacks; even cloud-based servers are not immune from being probed and subverted by hackers

Roark Pollock, Vice President at security firm Ziften

Image credited to NetEvents

As the number of endpoints proliferate — think Internet of Things — the odds of an endpoint being compromised and then used to gain access to the enterprise network and its assets only increases.

Which are the most vulnerable endpoints? Which need extra protection? All of them, especially devices running some flavor of Windows, according to Mike Spanbauer, Vice President of Security at testing firm NSS Labs. "All of them. So the reality is that Windows is where most targets attack, where the majority of malware and exploits ultimately target. So protecting your Windows environment, your Windows users, both inside your businesses as well as when they're remote is the core feature, the core component."

RoiAbutbul, Co-Founder and CEO of security firm Javelin Networks, agreed. "The main endpoints that need the extra protection are those

endpoints that are connected to the [Windows] domain environment, as literally they are the gateway for attackers to get the most sensitive information about the entire organization."
"From one compromised machine," he continued, "attackers can get 100 per cent visibility of the entire corporate, just from one single endpoint. Therefore, a machine that's connected to the domain must get extra protection."

Vulnerable IoT and Cloud

Scott Scheferman, Director of consulting at endpoint security company Cylance, is concerned about non-PC devices, as well as traditional computers. That might include the Internet of Things, or unprotected routers, switches, or even air-conditioning controllers. "In any organization, every endpoint is really important, now more than ever with the internet of Things. There are a lot of devices on the network that are open holes for an attacker to gain a foothold. The problem is, once a foothold is gained, it's very easy to move laterally and also elevate your privileges to carry out further attacks into the network."
At the other end of the spectrum is cloud computing, especially enterprise-controlled virtual servers, containers, and other resources configured as Infrastructure-as-a-Service (IaaS) and Platform-as-a-Service (PaaS). Anything connected to the corporate network is an attack vector, explained Roark Pollock, Vice President at security firm Ziften.
"We take a very holistic view of endpoint," Pollock said. "We'll talk about it as client to cloud, but I think of it as old-school client to server paradigm. And so we want to be on both ends of that wire and so we deploy on your traditional user client devices, so laptops, desktops, even virtualized desktops. Then we also install in the data center, whether it's physical servers, virtualized machines, virtual machines in that data center, even containers, and we can even deploy on those virtual machines, those virtual endpoints, even in an enterprise cloud application."
Microsoft, too, takes a broad view of endpoint security: "I think every endpoint can be a target of an attack. So usually companies start first with high privilege boxes, like administrator consoles onboard to service, but everybody can be a victim," said Heike Ritter, a Product Manager for Security and Networking at Microsoft.
The cloud is definitely a core concern, said Cylance's Scheferman. "Endpoints in the cloud are extremely important.Everybody's moved to the cloud, so a lot of your critical assets even live in the cloud and your critical data, your personal identifiable information (PII) personal health information (PHI), whatever it might be. You have to protect your endpoints from all factors in the cloud."

Context Is Everything

Many endpoint security products monitor endpoints and can raise alarms if

a breach is detected. Some tools focus on what's happening in this instant; others place incidents in a historical context, so that administrators and security response teams can see only what's going on, but where the problem began.

"Context truly is everything," said Scheferman. "We're starting to finally believe that in 2017.An event by itself means nothing, but an event coupled with other events gives you that context. When we're doing compromise assessments, we often look to build out what the context of the compromise was, in order to derive things like root cause analysis, where the attacker's gone.What they've been able to accomplish or not is also important, is knowing what they haven't been able to do.But you can't do that unless you have full context."

NSS Labs' Spanbauer agreed. "Ultimately you cannot act upon data and make it actionable unless you understand the context. Whether it's the delivery mechanic, what was going on, what was attempted, or what the user was doing at that specific moment in time.Without context, you can't act intelligently and solve the root problem."

Context is "actually very important, so if you think as numbers, statistics, they say it takes 200 days to discover a breach.You want to go back in time," said Microsoft's Ritter. "So sometimes you only learn today that this is an attack, that this is a certain pattern of an attack.So you now have new IOAs [Indicators of Attack], IOCs [Indicators of Compromise] reported by Windows Defender ATP. We will apply them like this new pattern back to up to six months of historical data, where now our customer can actually go back and investigate an attack that happened a little bit before."

Ziften's Pollock used a medical analogy for context providing a baseline: "Well for us, you have to both real time and contextual data, historical data.You don't go to the doctor today and find out you have cancer. You don't want to get in that situation and never have been to the doctor for a check-up in the last four years.You want to go to the doctor and have a check-up every year. The same thing from a security standpoint; it's about establishing a trend and being able to see what's happening over time."

Yet don't neglect the importance of real-time intelligence in helping reduce risk, warned John Wienschenk, General Manager of Enterprise Network and Application Security at Spirent Communications, arguing that you can never totally eliminate that risk. "You get the data that you have and at a snapshot in time, you prioritize those vulnerabilities that you have, whether it's on your mobile devices, your endpoint security, your infrastructure. And then you knock those down one at time.But realize that you'll never take your security risk to zero.That'll put you out of business."

Online, Offline: All Endpoints Need Protection

In an old-fashioned enterprise environment, nearly all endpoints were connected directly to the internal network, and unless they were powered off (like an employee's desktop computer over the weekend), they could be

monitors 24/7. What about in today's world, where endpoints are mobile, connected via cellular data or coffee-shop WiFi, or simply offline — but active? Those endpoints are even more vulnerable when traveling. They must be protected, and monitored by the CISO team so that breaches can be detected and responded to quickly. The same is true for virtual machines that can be spun up and then deactivated at any time. How are they protected?

Speaking to virtual machines, Ziften's Pollock said, "Our agent is part of the image of that virtual machine.So any time a virtual machine or a container spins up, we're already instantly part of that virtual device, so that virtual machine in the infrastructure. Immediately when it spins up, we start providing data feeds off of that image or that virtual machine.So we give you instant visibility for those virtual devices. Whether they spin up, if they stay up for a long time, if they get lost in your infrastructure, we're still monitoring and we know that those devices are there."

NSS Labs' Spanbauer added, "This is where advanced endpoint capabilities come into play.They self-monitor and certainly associate with the cloud for telemetry and other insights. But at the end of the day, you need to have a local autonomy, an intelligent mechanic on the endpoint itself to handle offline, or immediate reconnection capabilities. Meaning that if [the endpoint is] offline, comes back online, it won't have a chance to download new capabilities and come up-to-date.It has to be able to protect itself at the moment of being back online."

Finding Patient Zero

A breach is detected. An endpoint is found to be infected, and is isolated. Yet that endpoint may not the source of the original breach – it may simply be where hacker activity crossed over an alarm threshold. To stop the breach, and prevent it from reoccurring, it's vital to find the root cause of the vulnerability, also known as Patient Zero. That user, device or application can be tricky to identify.

"For us, it starts even before you get to Patient Zero," said Ziften's Pollock. "It's about good security hygiene and being able to prevent as many of those treats as possible by maintaining your hygiene. But then once you identify a threat in that environment, it's about being able to immediately provide context so that the security operations teams know immediately what they're looking at, what device, what the user is."

Kowsik Guruswamy, CTO of security firm Menlo Security, said that the data is there to identify breaches, even if technologies like his company's isolation platform stop any harm from being done, or any data from being exfiltrated. "The best analogy I would tell you is I tell customers that we're giving them a bulletproof vest.So there are no bullets that are going to touch them at all. However, many customers still want to know where the bullets are coming from and what types of bullets are hitting at them. So while we're isolating and making the problem go away, we still use threat

intelligence and other techniques, from a purely reporting and forensics perspective, to tell the users what type of bullets came at them."
"That's the challenge. So whether it's antivirus or it's malware or anything else, there's always one person that gets hit with the attack first," said Spirent's Weinschenk. "Then once it gets hit, then you create the inoculations and everyone gets to know whether they're susceptible or not.So the best thing that you can do is once you realize that could have that issue, then you need to take proactive action, either blocking those vulnerabilities or fixing the code base" if it was a software defect that caused the vulnerability.
Microsoft's Rittrer added, "There will be an alert, of course, either in the SIEM [security incident event manager] or they go to our portal. So after they got an alert, they go and investigate in our portal. We raise alerts based on behavioral events that we collected from the box and our tool gives them all the investigation capabilities. We show the process tree, the time, the user, the machine, where did the file go, where it came from.So it gives you the entire visibility into what happened on the endpoint with the behavioral context.
SecureLink is the biggest security-specific reseller and managed security services provider (MSSP) in Europe. Stefan Lager, SecureLink's Vice President of Services, added that "The important thing that many customers lack today and the statistics show that you can be infected for many months before detecting it, is because they don't have the visibility today. We need to have visibility almost going on at the endpoint, in the network and on the different logs that we collect. If you don't have that, it's very hard to track down exactly what happened and what was the root cause."

Solid Ideas for Endpoint Protection

Many companies offer solutions for endpoint protection, whether that endpoint is physical or virtual, mobile or in a data center or in the cloud. Each company has a different vision. For example, Javelin Networks focuses on protecting Active Directory, an essential component of a Windows domain network. Active Directory can be used by hackers to learn about network resources, and target future attacks.
"Acknowledging the fact that the first thing that the attackers will do after they get a foothold on a machine that is connected to the [Windows] domain, they will try to learn about the environment using Active Directory attacks to steal domain credentials," said Javelin Networks' Abutbul. "Our solution understands that methodology and mask that entire information and control the attacker perception at the endpoint itself."
He continued, "At the end of the day, the attackers will never be able to get to the real information that Active Directory contains. So the moment they will act upon a machine that is not a real machine and was the masked [unclear] we projected to the endpoint, that's game over for them. And we

will be able to catch them right at the endpoint itself, right at the point of breach, before they move further into the organization."
Ziften takes a much more holistic view of the endpoint, said Pollock. "Whether it's a user device connected to the network, a user device offline connected in a coffee shop or working from home, we can provide intelligence on those devices.We even continue to monitor devices that are offline completely. We cache that information and then we upload it when they get back online.We also work in the data center, we also work in cloud environment.We actually give you the ability to look back over a period of time and understand trends, understand behaviors, whether it's application and device behaviors or user behavior, over a period of time."
Fast response for zero-day vulnerabilities, that's the trick, said Cylance's Scheferman. "Cylance responds to many incidents per year. In fact we found the OPM breach[U.S. Office of Personal Management], which a lot of people have read about recently.We were able to stop that malware.The reason we were able to do that is because of our predictive technology, combined with a lot of automation expertise."
In fact, he added, "Our predictive technology allows us to identify malware that may have been complied a year prior.And we're blocking it a year before there's any identification of that malware in the industry whatsoever.In the context of instant response, it allows us to use our technology to immediately identify and contain a threat.That's why we call our practice incident containment instead of incident response."

Protect the Endpoints. Or Else.
Every endpoint represents a potential enterprise vulnerability. Mobile phone, notebook computer, datacenter server, virtual container in the cloud, the IoT, and even industrial equipment. It's not a question of "if" endpoints will be attacked, but "when." The challenge for enterprises is to be able to prevent, detect and respond to those breaches. The technologies and service providers above have answers. It's time more organizations talked to them.

To see the video, please visit:

https://youtu.be/pNP0bI7T8R4